IN THE CLAIMS:

Please amend the claims as follows:

31. (Currently Amended) A method of operating a file server, said method including steps of:

identifying a ~~first~~ file on said file server with a first security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server; and

enforcing said first security style for all accesses to said ~~first~~ file including accesses in another one of said plurality of security styles.

32. (Previously Presented) A method as in claim 31, wherein said plurality of security styles includes a Windows NT security style.

33. (Previously Presented) A method as in claim 31, wherein said plurality of security styles includes a Unix security style.

34. (Currently Amended) A method as in claim 31, wherein said enforcing step enforces said security style for all accesses to the ~~first~~ file regardless of the security style associated with the entity who seeks access to the ~~first~~ file.

35. (Currently Amended) A method as in claim 31, including the steps of:

associating said ~~first~~ file with a subset of files in a file system; and

limiting said subset of files to a security subset of said plurality of security style;

wherein attempts to set permission in said subset of files are restricted to said security subset.

36. (Previously Presented) A method as in claim 35, wherein said security subset includes a Windows NT security style.

37. (Previously Presented) A method as in claim 35, wherein said security subset includes a Unix security style.

38. (Previously Presented) A method as in claim 35, further comprising the step of caching associations and limits for the subset of files for future use.

39. (Currently Amended) A method as in claim 31 [[35]], wherein the steps of identifying and enforcing further comprise mapping permissions in said first security style to a second security style, and wherein said mapping ~~associating and limiting~~ can be performed dynamically ~~, associated with a specific attempt to access a file,~~ or statically ~~, not associated with a user or specific attempt to access a file~~.

40. (Currently Amended) A method of operating a file server, said method including steps of

identifying a ~~first~~ file on said file server with a first security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server;

enforcing said first security style for all accesses to said file server including accesses in another one of said plurality of security styles; and

identifying said ~~first~~ file with a second security style selected from among the plurality of security styles in response to a file server request.

41. (Currently Amended) A method as in claim 40, including steps of associating said second security style with a file server request for setting permissions for said ~~first~~ file when said file server request is successful.

42. (Currently Amended) A method as in claim 40, wherein said ~~first~~ file is associated with said second security style regardless of the security style previously associated with said ~~first~~ file.

43. (Currently Amended) A file server including:

a set of files available on said file server, each said file having an associated security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server;

wherein said file server enforces said associated security style for all accesses to said file including accesses in another one of said plurality of security styles.

44. (Previously Presented) A file server as in claim 43, wherein said plurality of security styles includes a Windows NT security style.

45. (Previously Presented) A file server as in claim 43, wherein said plurality of security styles includes a Unix security style.

46. (Previously Presented) A file server as in claim 43, including

a subtree of files in said file system associated with a security subset of said plurality of security styles;

wherein said file server restricts attempts to set permissions in said subtree to said security subset.

47. (Previously Presented) A file server as in claim 46, wherein said security subset includes a Windows NT security style.

48. (Previously Presented) A file server as in claim 46, wherein said security subset includes a Unix security style.

49. (Previously Presented) A file server as in claim 43, wherein said file server is capable of altering the security style associated with said file in response to a file server request.

50. (Currently Amended) A file server as in claim 49 [[69]], wherein said file server is capable of altering the security style associated with said file in response to a file server request when said file server request is successful.

Claims 51 to 53 (Cancelled)

54. (Previously Presented) In a file server having a plurality of files and a security style associated with each file, said security style being selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server, a data structure associating a security subset of said plurality of security styles with a subtree of said files available on said file server.

55. (Previously Presented) A data structure as in claim 54, wherein said security subset includes a Windows NT security style.

56. (Previously Presented) A data structure as in claim 54, wherein said security subset includes a Unix security style.

57. (New) A method as in claim 1, wherein said step of enforcing further comprises translating a user identification associated with said accesses to said first security style or translating access control limits for said file to a second security style associated with said accesses.

58. (New) A file system as in claim 43, wherein said file server enforces said associated security style by translating a user identification associated with said accesses to said associated security style or by translating access control limits for said file to a second security style associated with said accesses.